CS 88: Security and Privacy

17: Network Security, DNS

11-01-2022

slides adapted from Dave Levine, Jim Kurose

Reading Quiz

How A Small ISP in Pennsylvania Tanked a Big Chunk of the Web on Monday

And how Verizon apparently made it much worse.

Network Security!

Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud

Global Botnets Shut Down Following Arrests

A 13-count indictment was unsealed today in federal court in Brooklyn charging Aleksandr Zhukov, Boris Timokhin, Mikhail Andreev, Denis Avdeev, Dmitry Novikov, Sergey Ovsyannikov, Aleksandr Isaev and Yevgeniy Timchenko with criminal violations for their involvement in perpetrating widespread digital advertising fraud. The charges include wire fraud, computer intrusion, aggravated identity theft and money laundering. Ovsyannikov was arres
month in Bulgaria; and Timchenko was arr

Alleged mastermind behind attack that 'almost broke the internet' goes on trial

Sven Olaf Kamphuis says he will not appear in court in Netherlands to face charges he arranged 2013 attack that slowed web traffic worldwide

Sven Olaf Kamphuis has been accused of launching an unprecedented cyberattack that reportedly "almost broke the internet" in 2013. Photograph: Alamy

Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

Dennis Fisher *October 31,*

The attacker who penetrated the Dutch CA DigiNotar last year had complete control
eight of the company's certificate-issuing servers during the operation and he may al
have issued some rogue certificates that have not yet been identified.

What is the goal of a network?

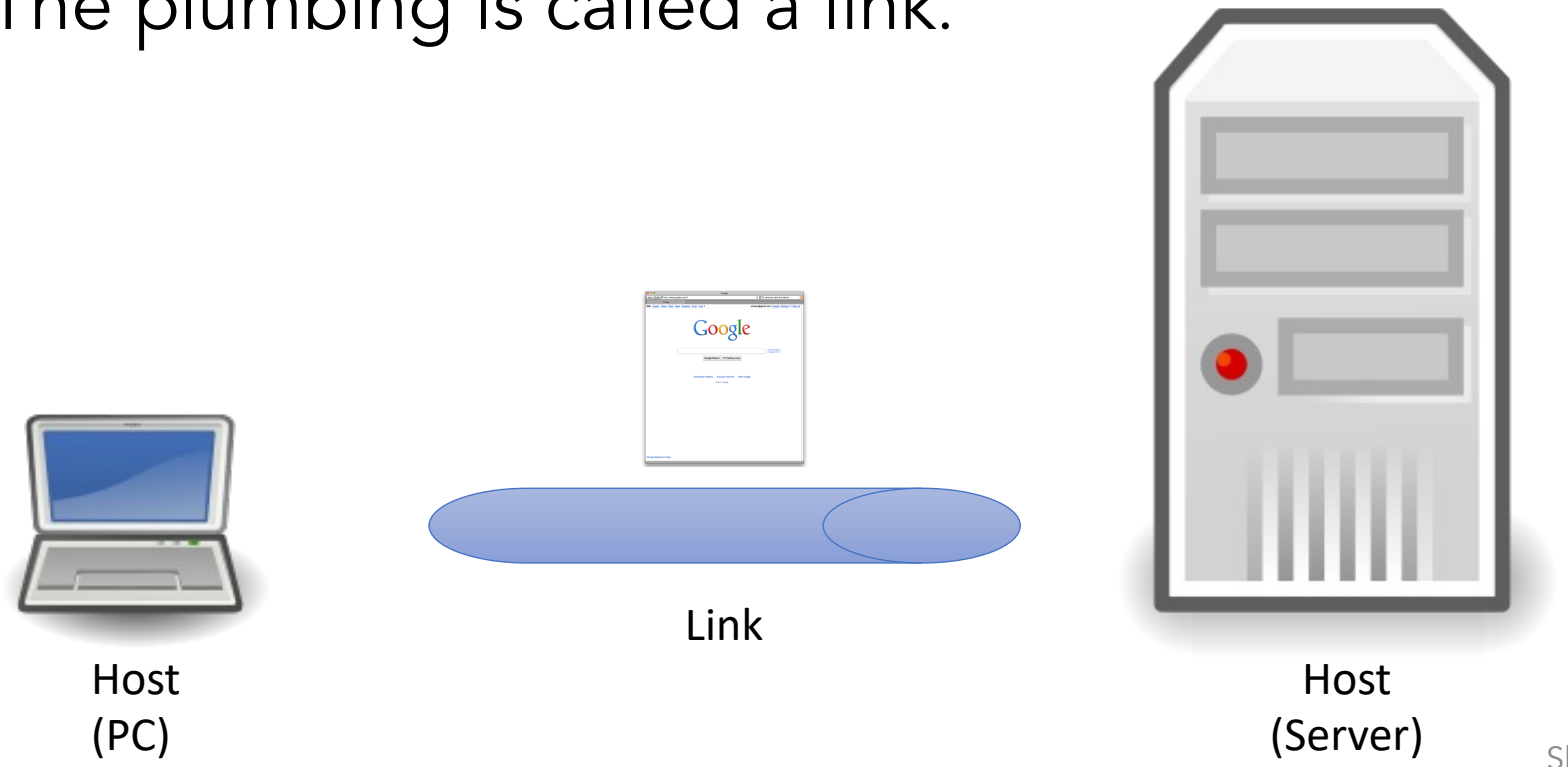
- Allow devices communicate with one another and coordinate their actions to work together.

- Piece of cake, right?

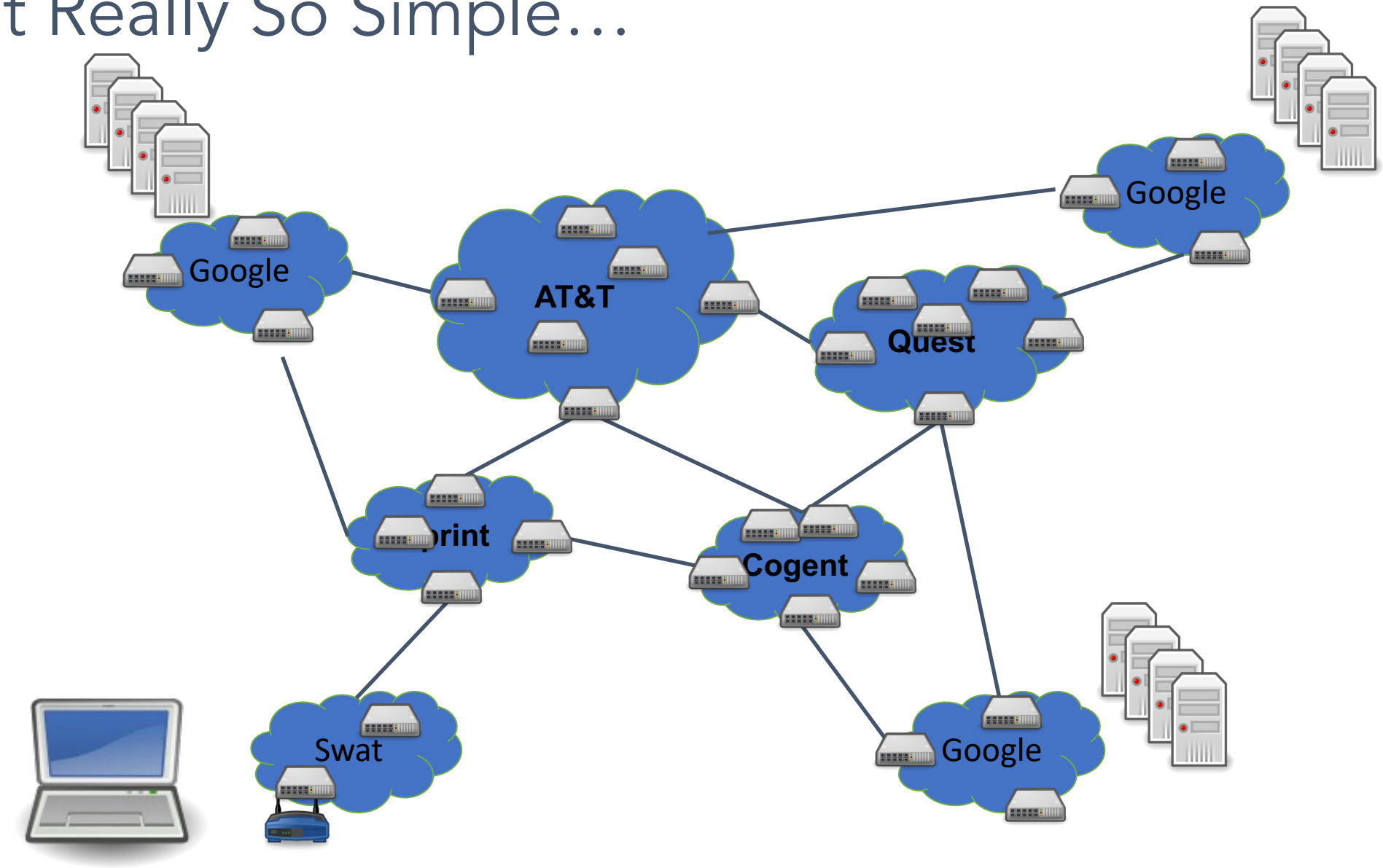
A "Simple" Task

Send information from one computer to another

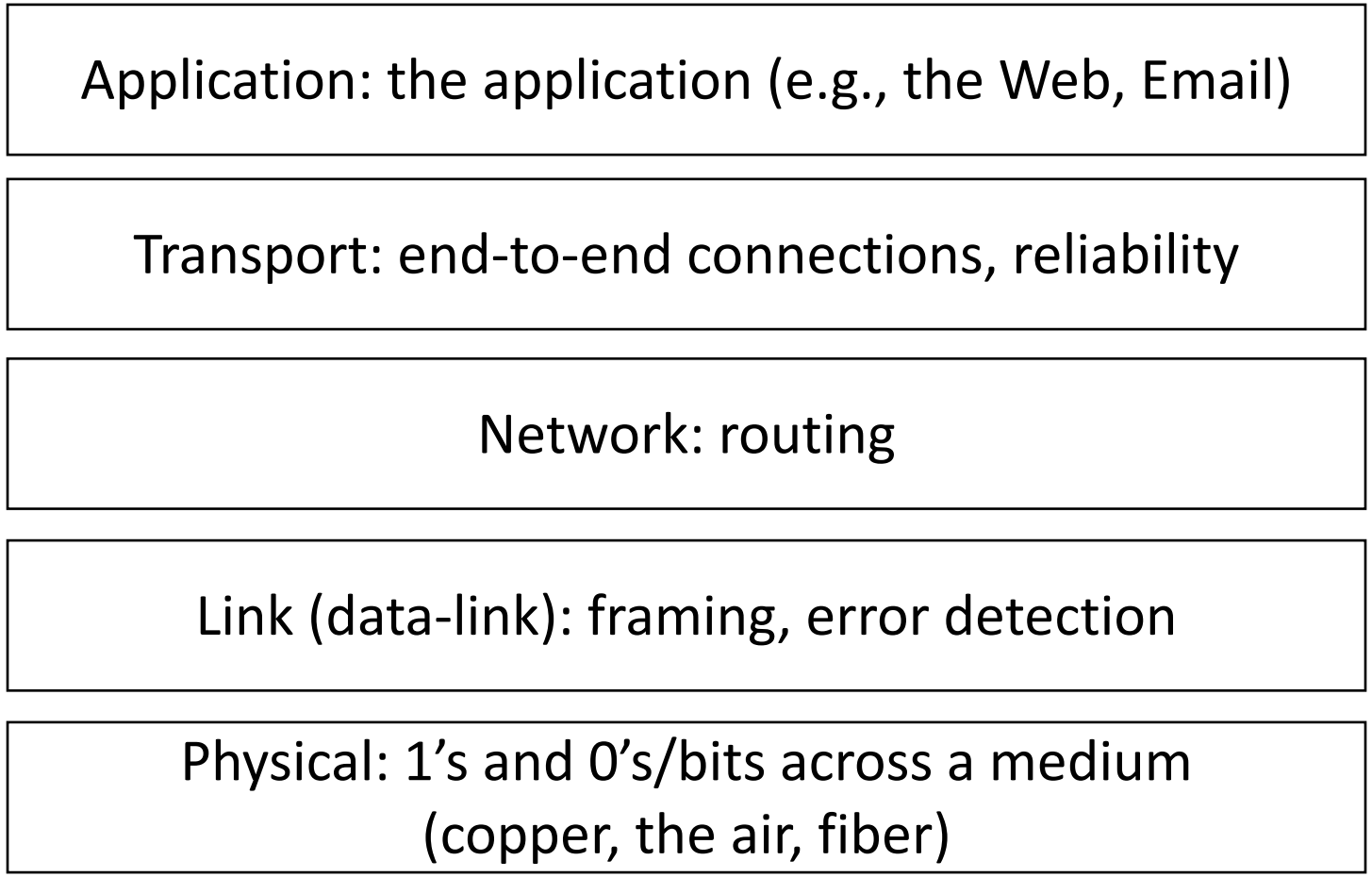
- hosts: endpoints of a network
- The plumbing is called a link.



Not Really So Simple…

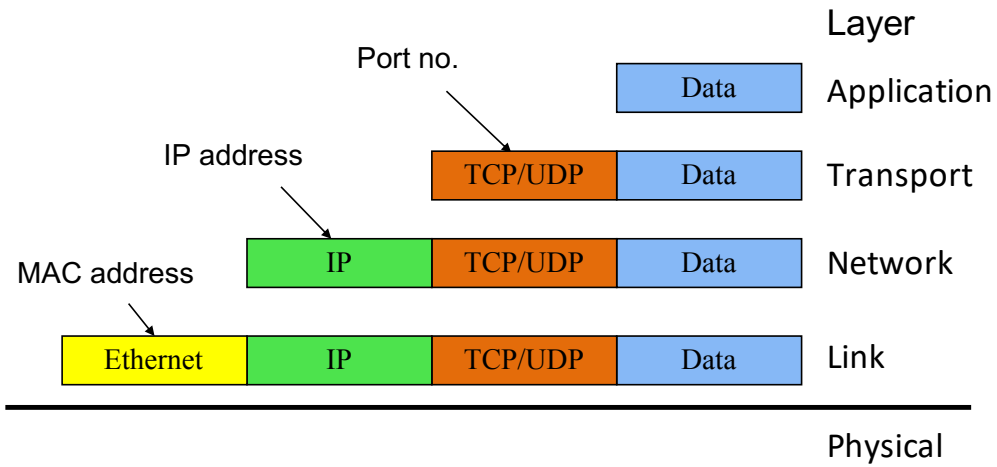


Five-Layer Internet Model



Application Layer (HTTP, FTP, SMTP, Skype)

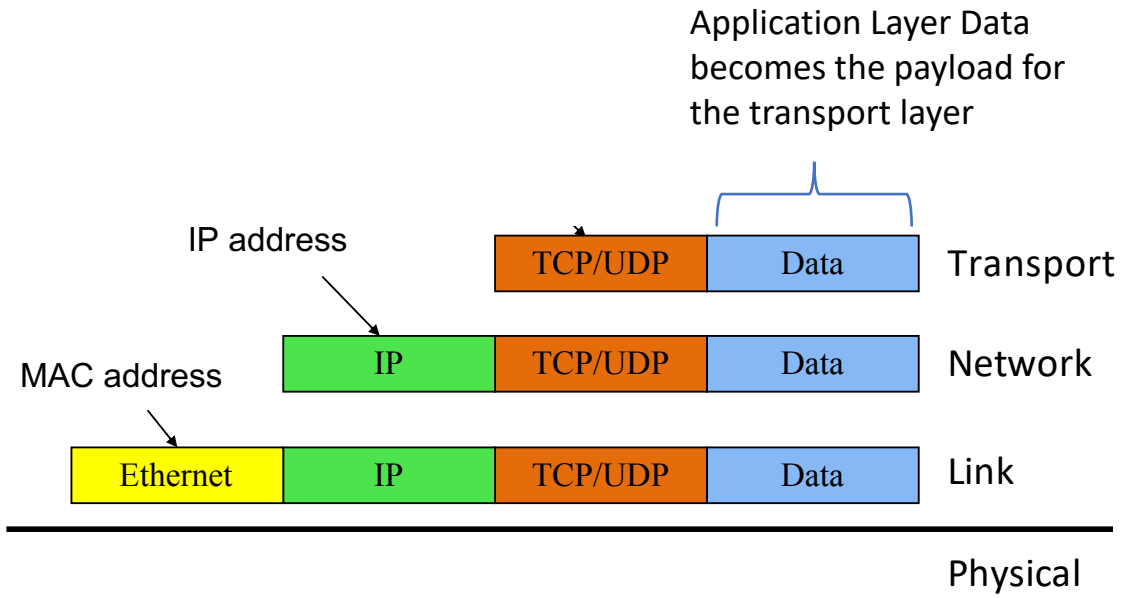
- Does whatever an application does!



Transport Layer (TCP, UDP)

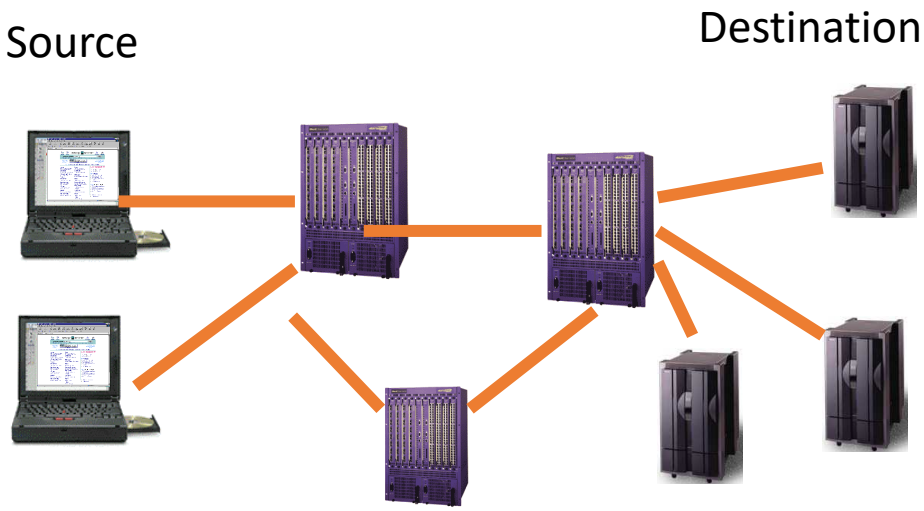
- Provides
  - Ordering
  - Error checking
  - Delivery guarantee
  - Congestion control
  - Flow control

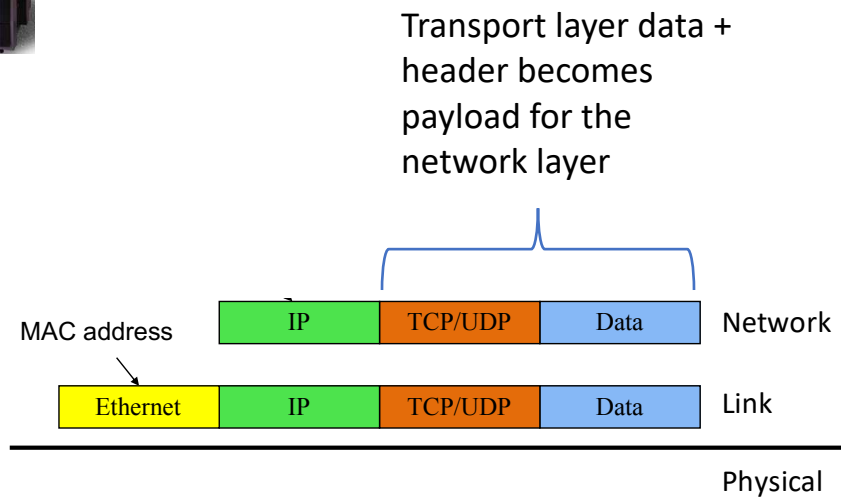
- Or doesn't!



Network Layer (IP)

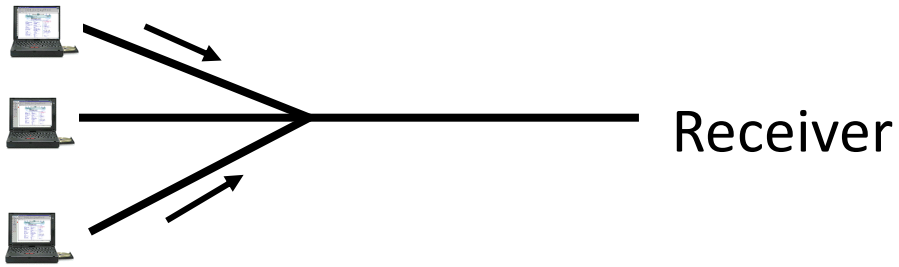
- **Routers**: choose paths through network



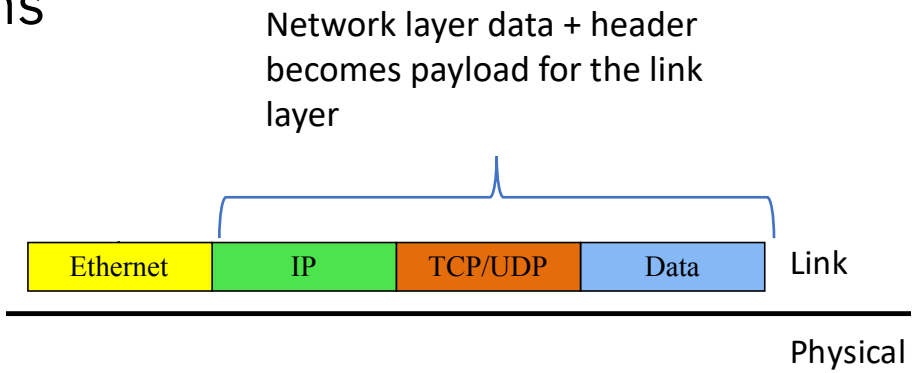


Link Layer (Ethernet, WiFi, Cable)

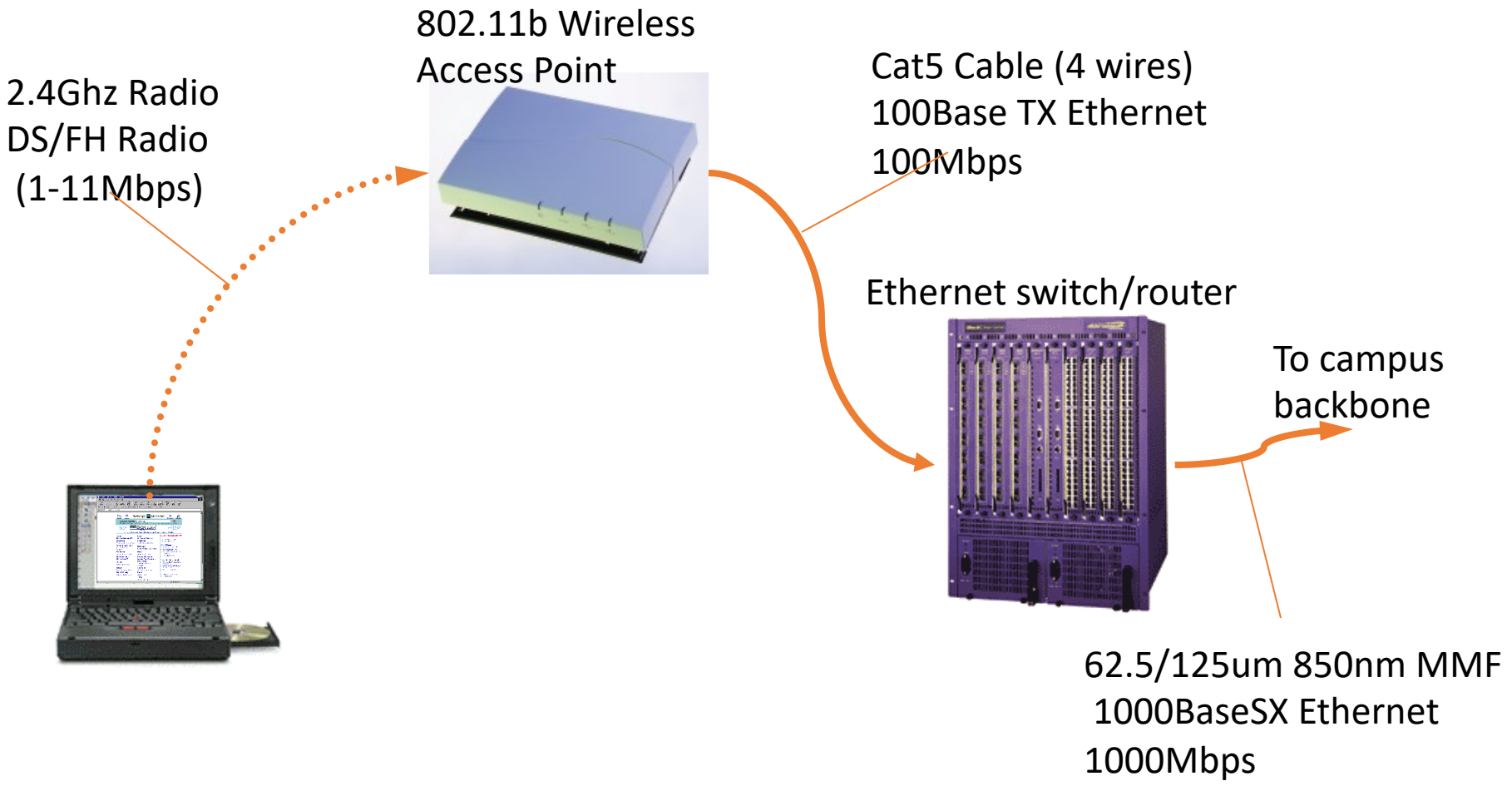
- Who's turn is it to send right now?
- Break message into frames
- Media access: can it send the frame now?



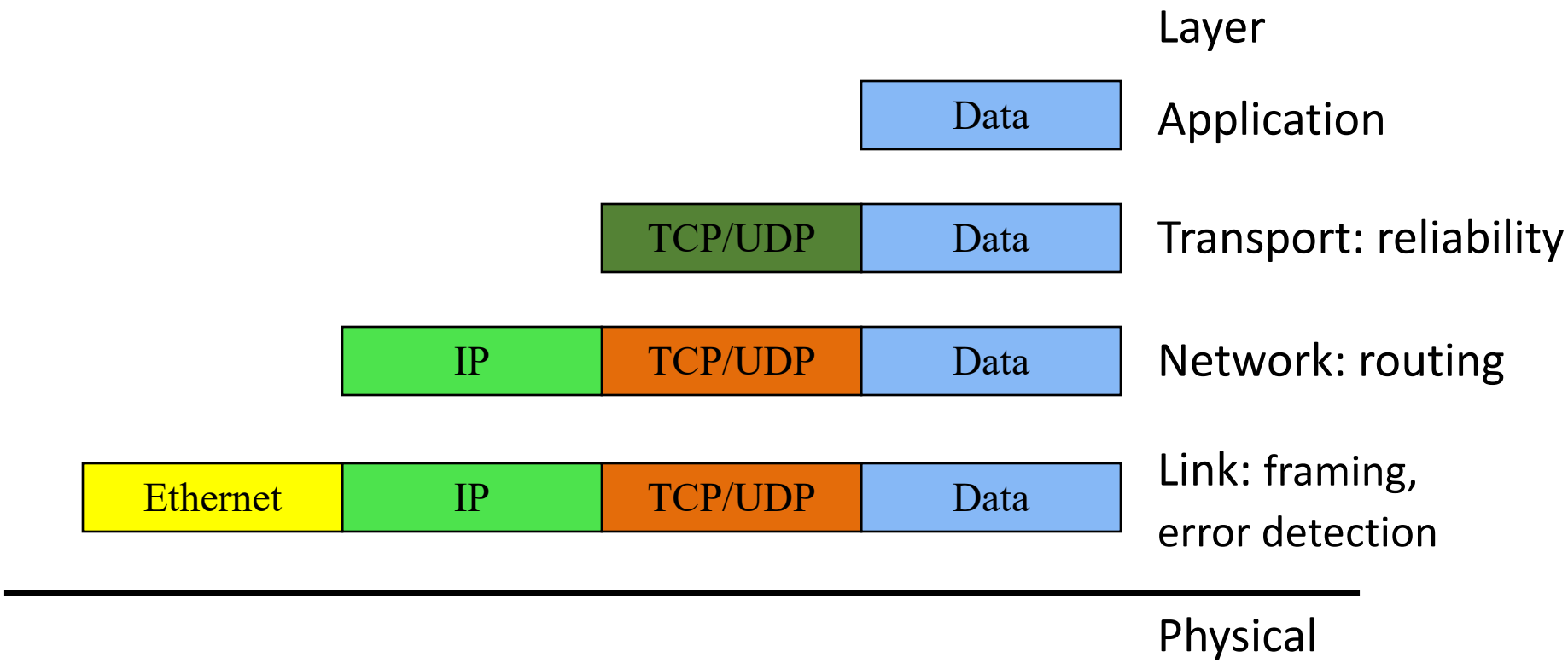
- Send frame, handle "collisions"



Physical layer – move actual bits! (Cat 5, Coax, Air, Fiber Optics)



Layering and encapsulation

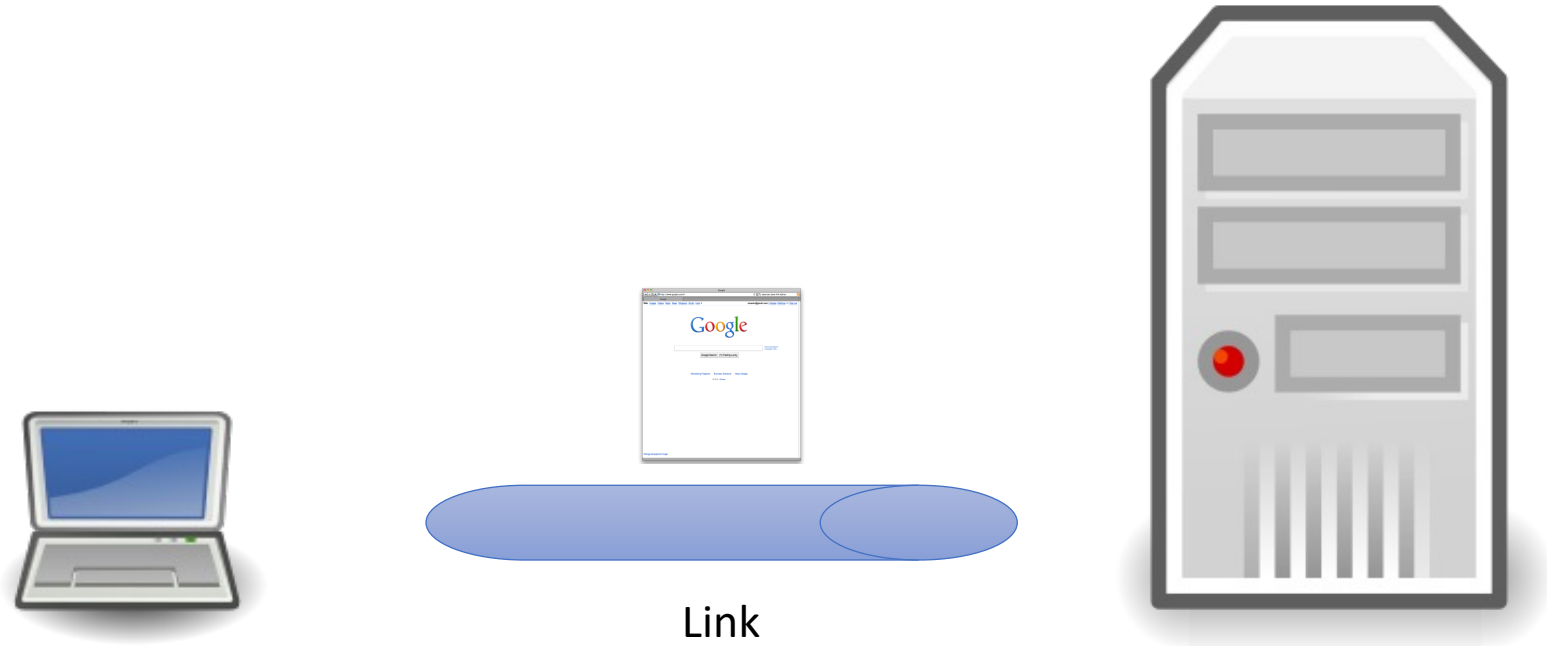


Layering: Separation of Functions

- explicit structure allows identification, relationship of complex system's pieces
  - layered reference model for discussion
  - reusable component design
- modularization eases maintenance
  - change of implementation of layer's service transparent to rest of system,
  - e.g., change in postal route doesn't effect delivery of lette

A "Simple" Task

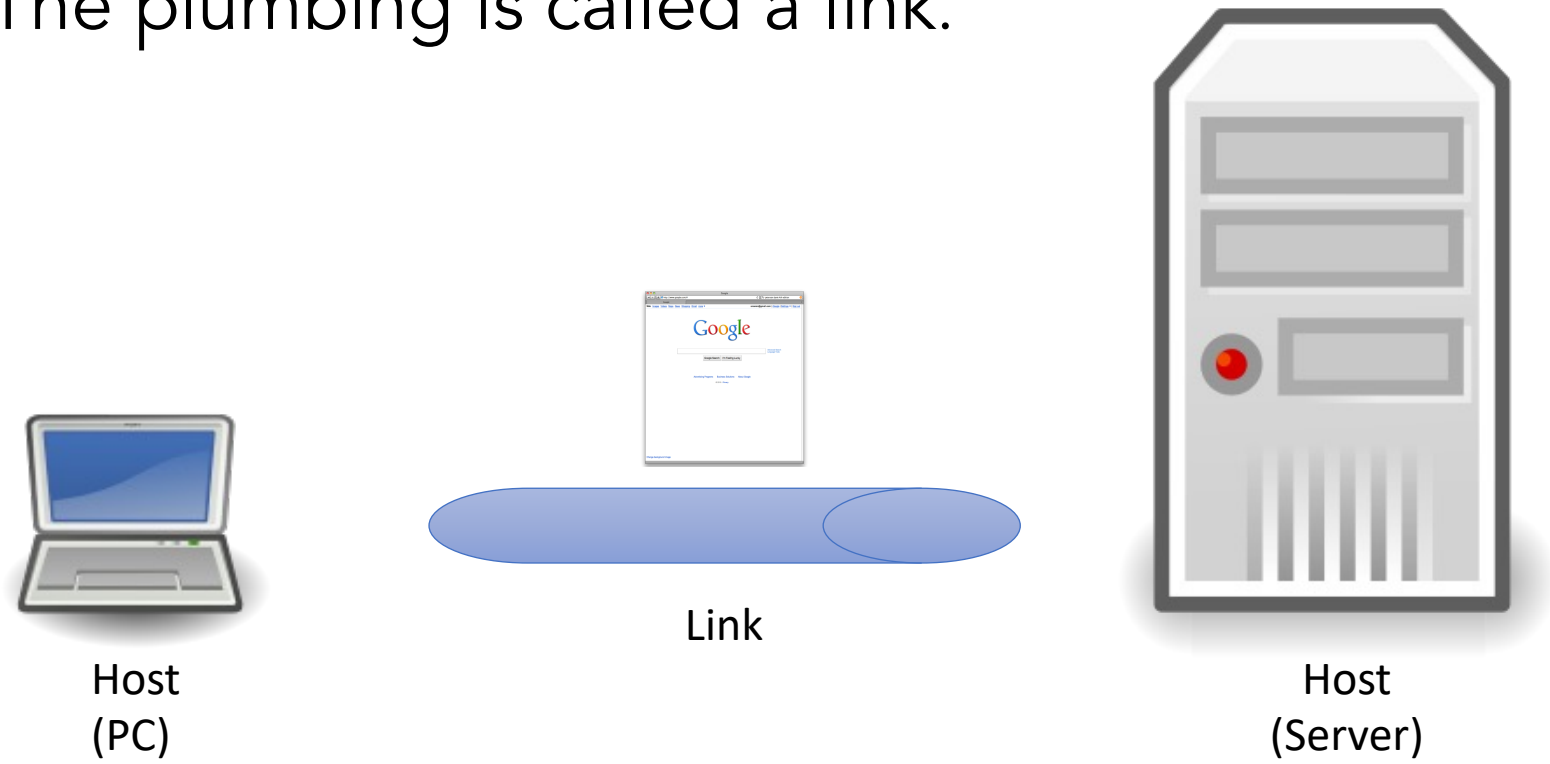
Send information from one computer to another



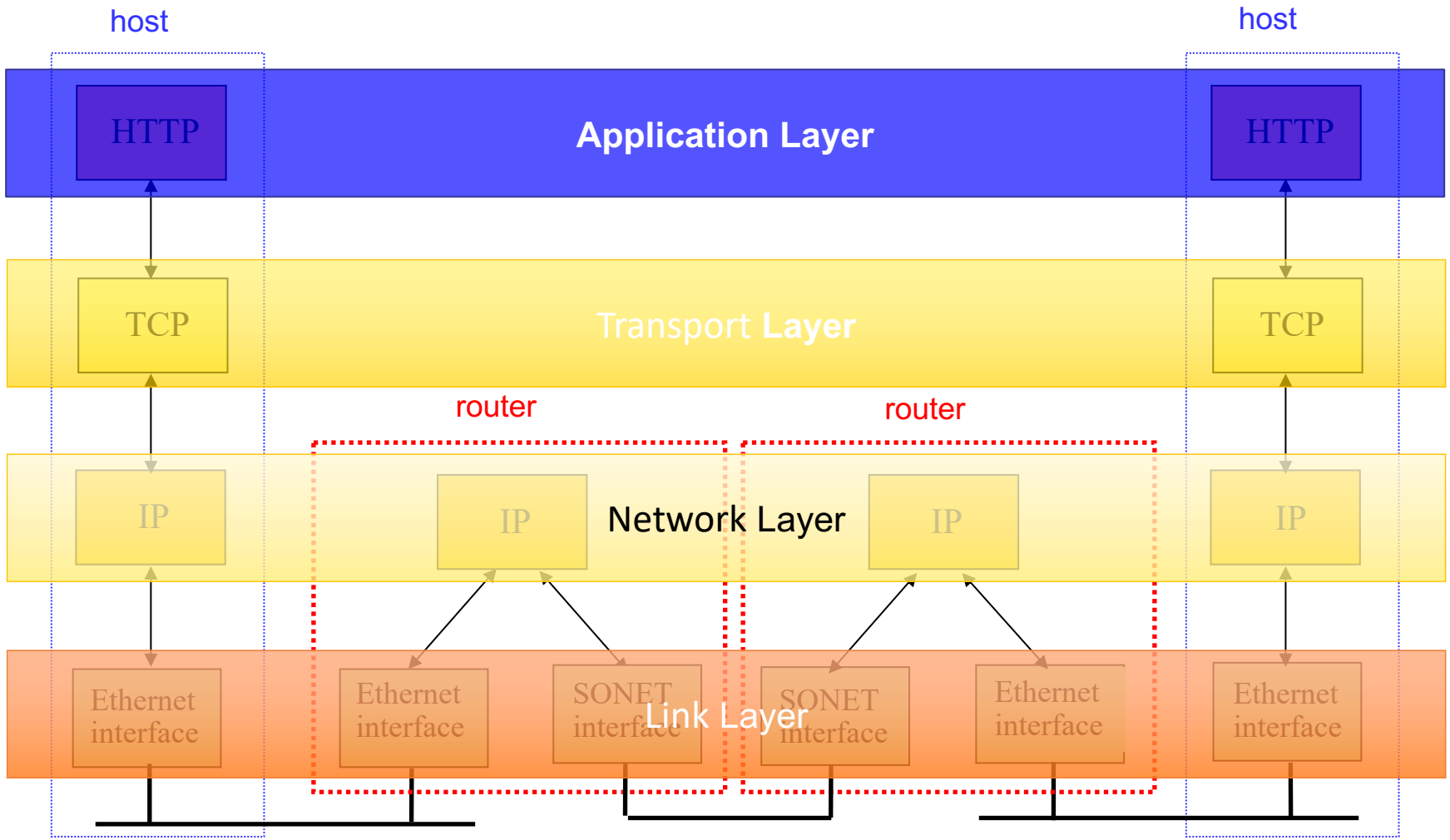
A "Simple" Task

Send information from one computer to another

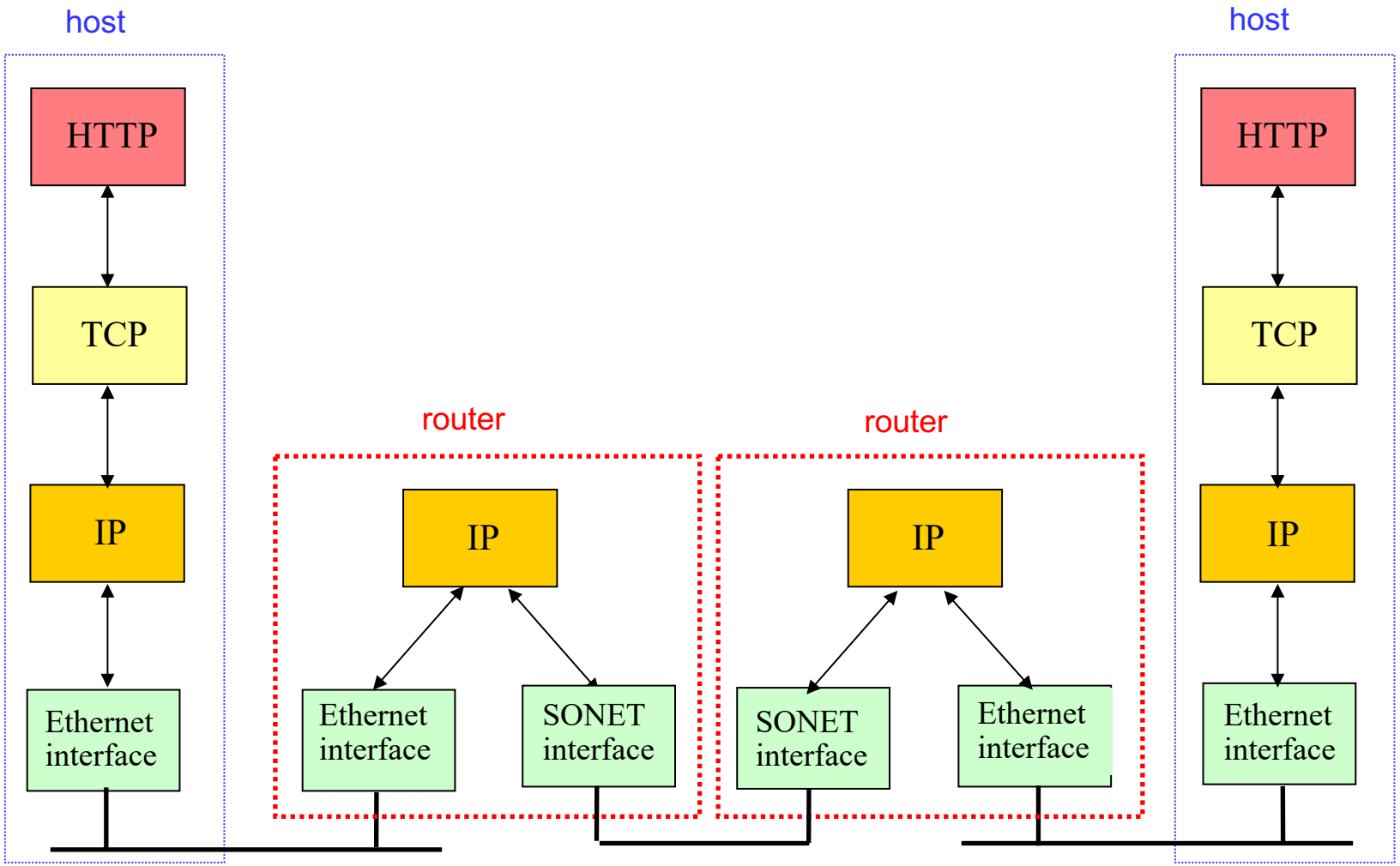
- hosts: endpoints of a network
- The plumbing is called a link.



TCP/IP Protocol Stack



TCP/IP Protocol Stack



DNS: Domain Name System

People: many identifiers:

- name, swat ID, SSN, passport #

Internet hosts (endpoints), routers (devices inside a n/w):

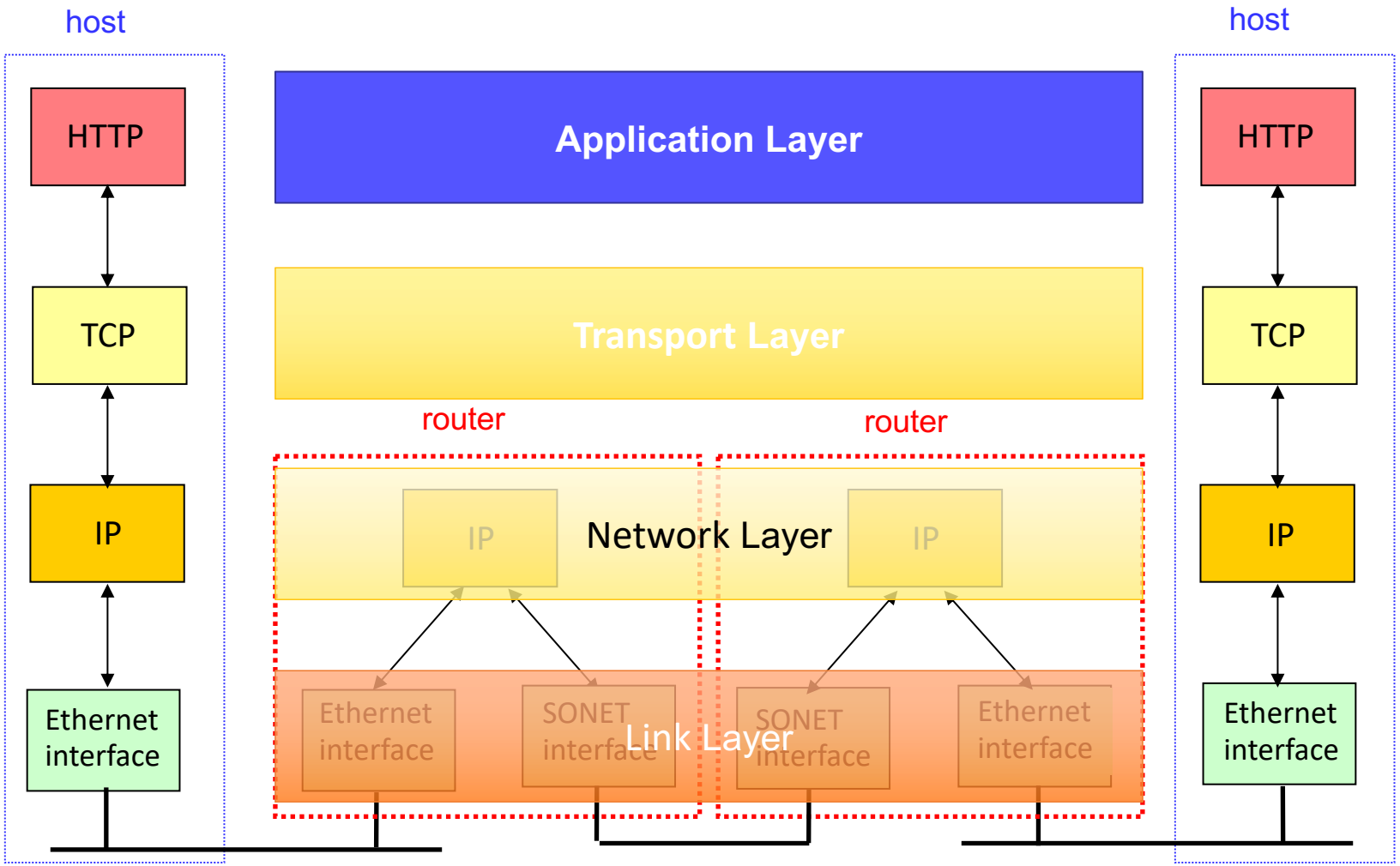
- “name”, e.g., www.google.com - used by humans
- IP address (32 bit) - used for addressing packets

How do we map between IP address and name, and vice versa ?

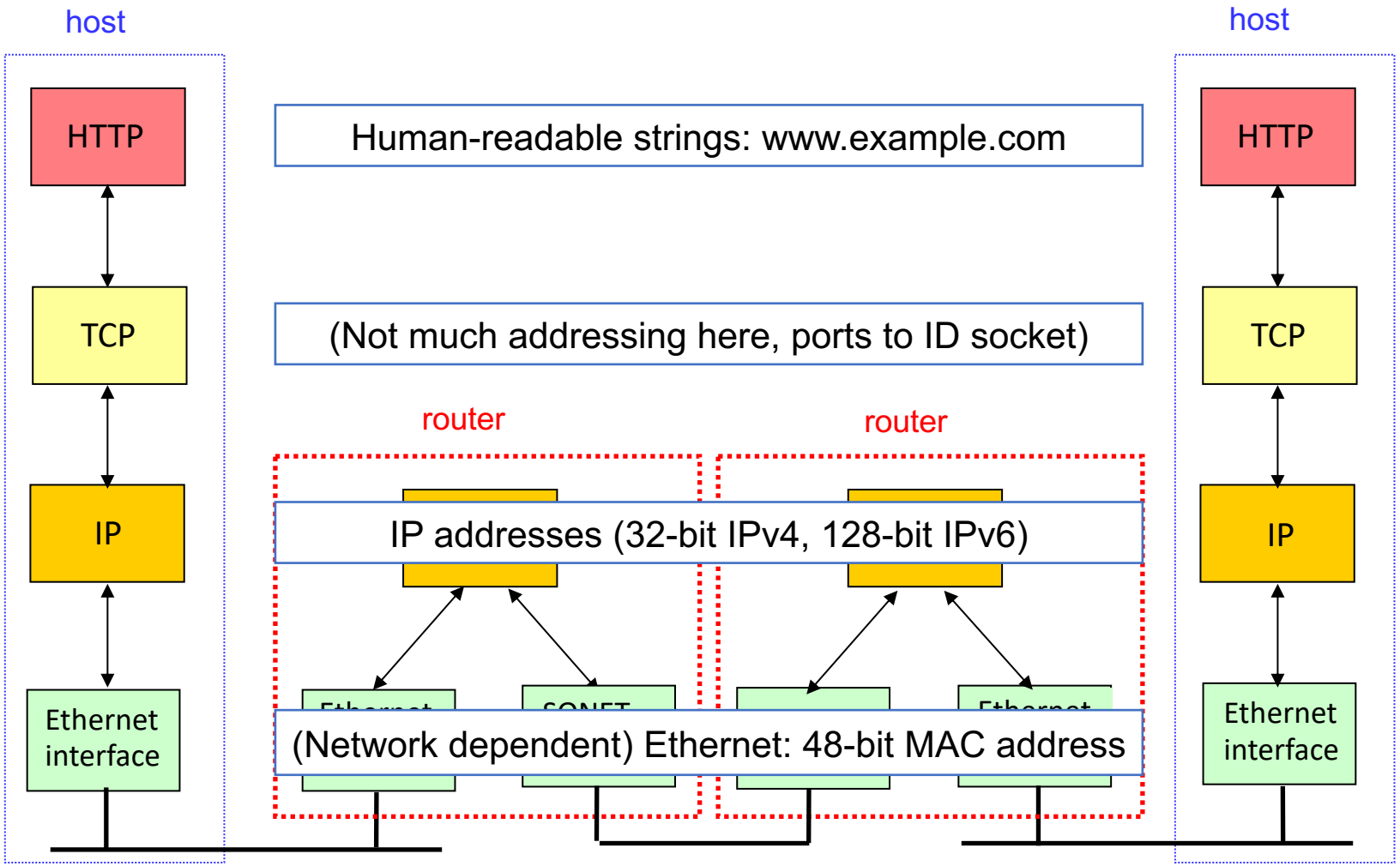
DNS: Application Layer Protocol

- distributed database
  - implemented in hierarchy of many name servers.
- application-layer protocol:
  - hosts communicate to name servers
  - resolve names → addresses
- *note: core Internet function, implemented as application-layer protocol*

Where


host
host
HTTP
TCP
IP
Ethernet interface
Application Layer
Transport Layer
router
router
IP
Network Layer
IP
Ethernet interface
SONET interface
Link Layer
SONET interface
Ethernet interface
HTTP
TCP
IP
Ethernet interface

Recall: TCP/IP Protocol Stack



Goals of DNS

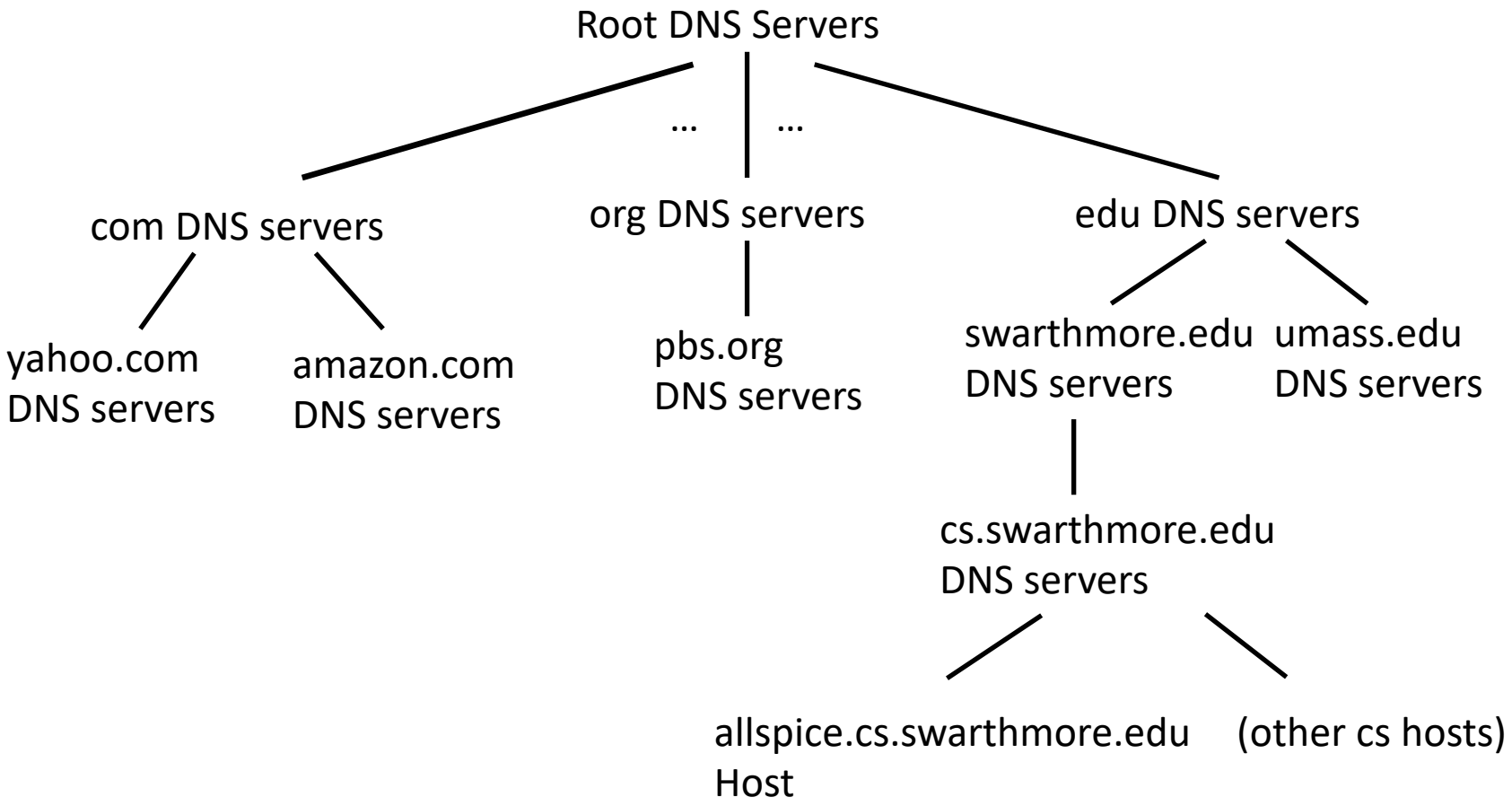
A wide-area distributed database

Possibly biggest such database in the world!

Goals

- Scalability; decentralized maintenance
- Robustness
- Global scope
- Names mean the same thing everywhere
- Distributed updates/queries
- Good performance

DNS: a distributed, hierarchical database

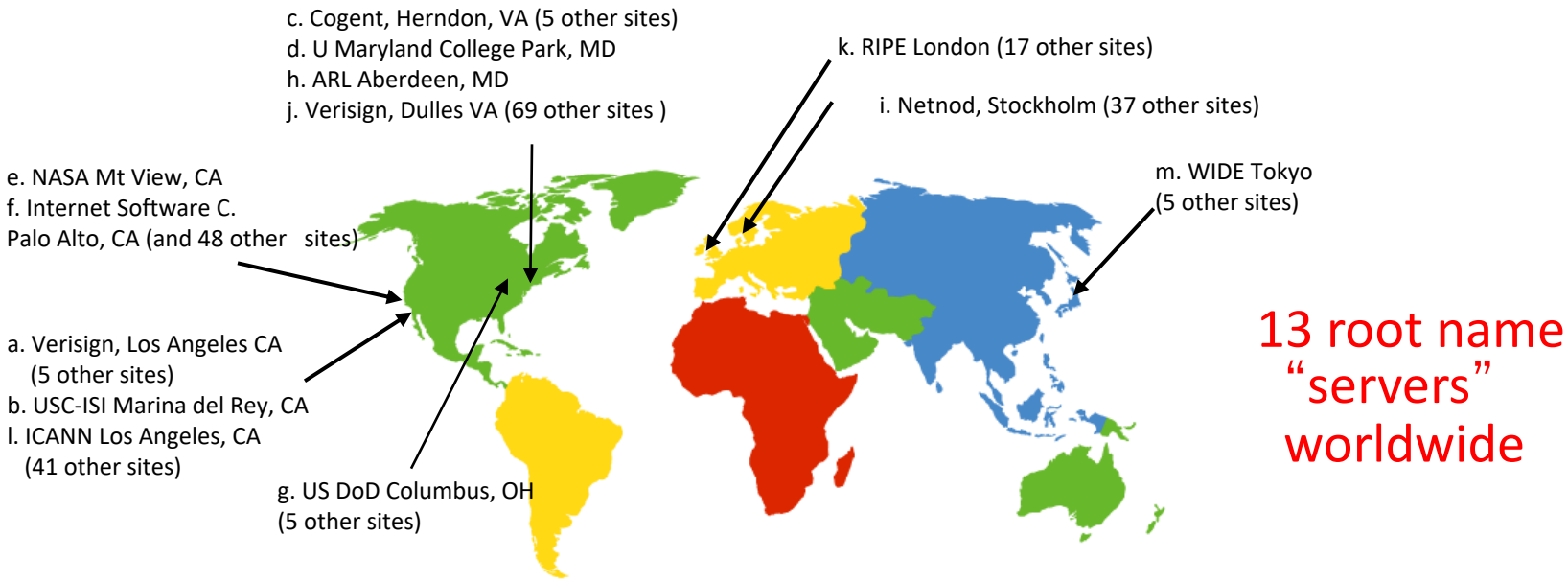


- allspice.cs.swarthmore.edu.

Nameless root,
Usually implied.

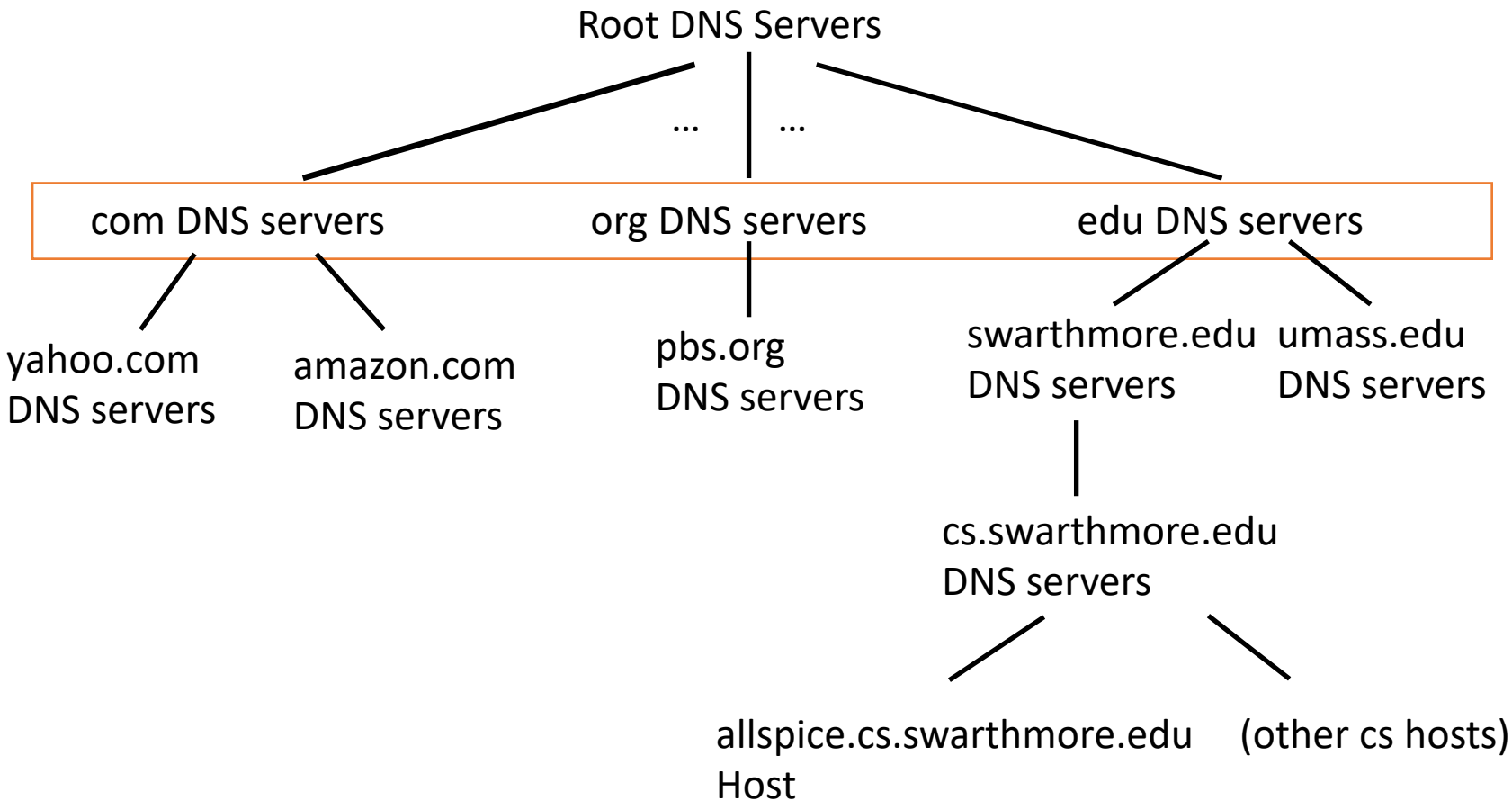
DNS: Root Name Servers

- Root name server:
  - Knows how to find top-level domains (.com, .edu, .gov, etc.)
  - How often does the location of a TLD change?
  - approx. 400 total root servers
  - Significant amount of traffic is not legitimate

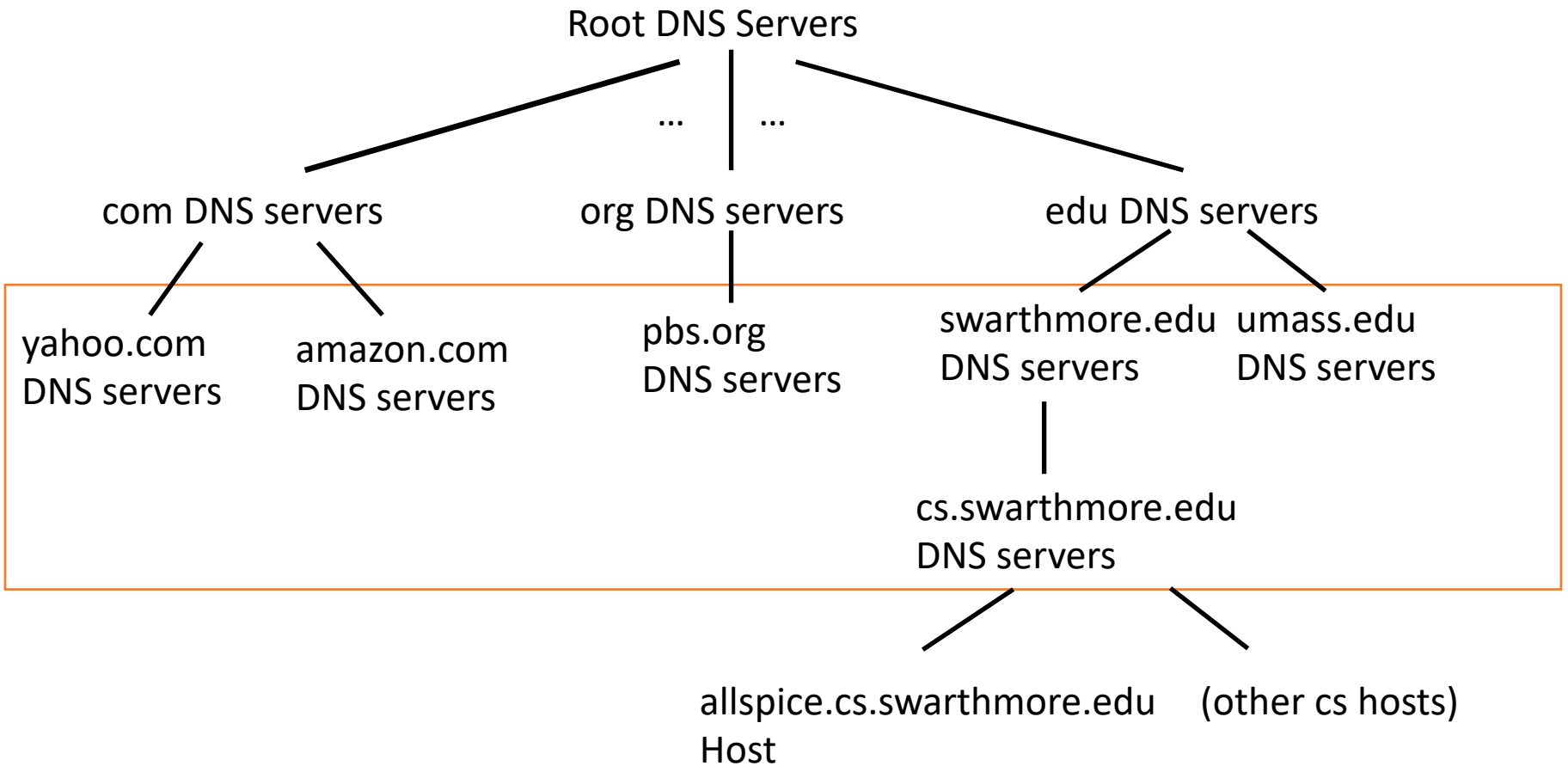


13 root name "servers" worldwide

DNS: a distributed, hierarchical database



DNS: a distributed, hierarchical database



Authoritative Servers

Authoritative DNS servers:

- Organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
- Can be maintained by organization or service provider, easily changing entries
- Often, but not always, acts as organization's local name server (for responding to look-ups)

Local DNS Name Server

- Each ISP (residential ISP, company, university) has (at least) one
  - also called “default name server”

- When host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

Uses of DNS

Hostname to IP address translation

- Reverse lookup: IP address to hostname translation

Host name aliasing: other DNS names for a host

- Alias hostnames point to canonical hostname

Email: look up domain's mail server by domain name

Different DNS Mappings

1-1 mapping between domain name and IP addr

- www.cs.cornell.edu maps to 132.236.207.20

Multiple domain names maps to the same IP addr

- eecs.mit.edu and cs.mit.edu both map to 18.62.1.6

Single domain name maps to multiple IP addrs

- aol.com and www.aol.com map to multiple IP addrs

Some valid domain names don't map to any IP addr

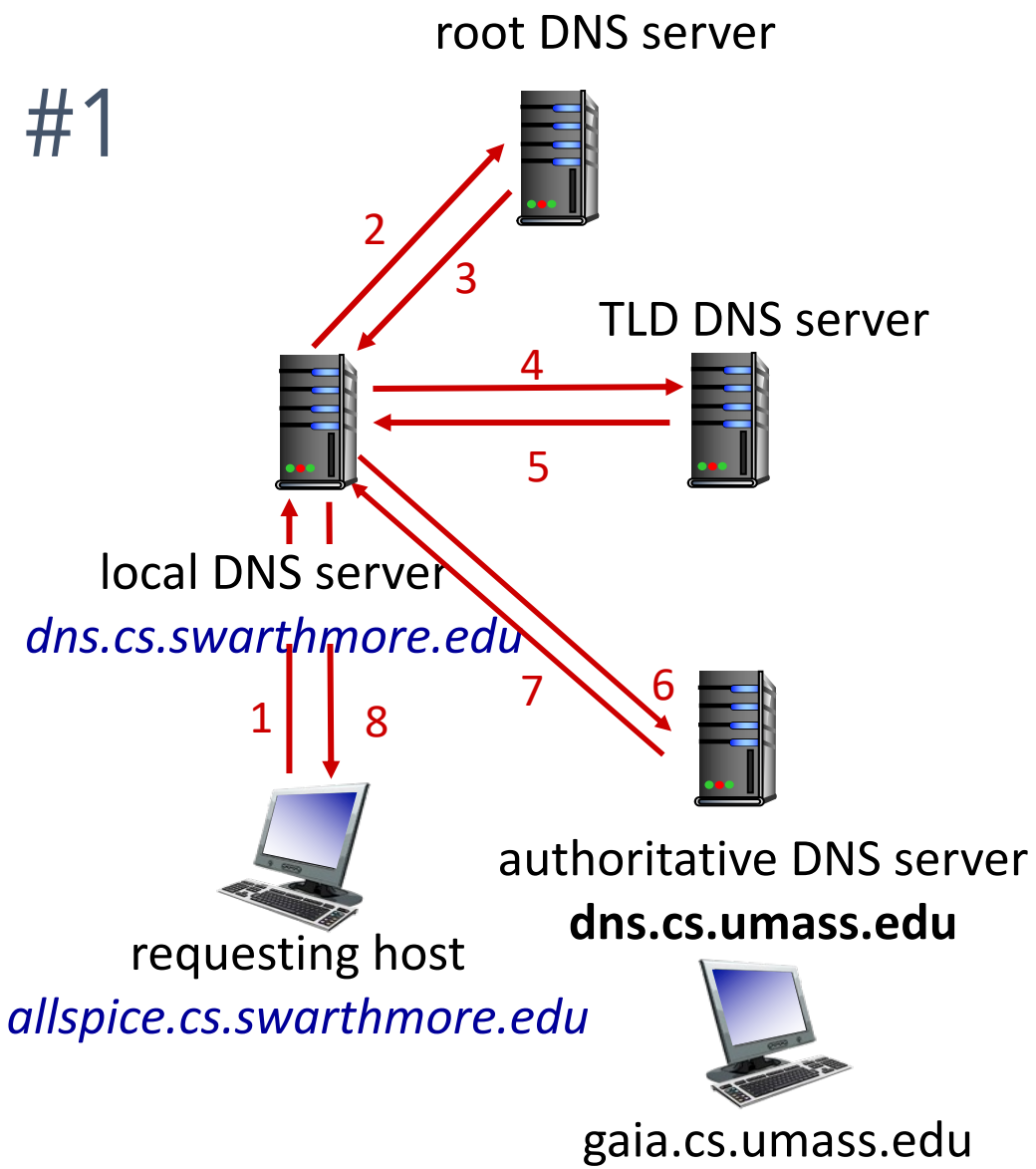
- cmcl.cs.cmu.edu

DNS name resolution example #1

- allspice wants IP address for gaia.cs.umass.edu

iterative query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



How many answers
Time to live in seconds
How many additional records?

```
$ dig @a.root-servers.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57494
;; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.freebsd.org.               IN      A

;; AUTHORITY SECTION:
org.                    172800 IN      NS      b0.org.afilias-nst.org.
org.                    172800 IN      NS      d0.org.afilias-nst.org.

;; ADDITIONAL SECTION:
b0.org.afilias-nst.org.    172800 IN      A       199.19.54.1
d0.org.afilias-nst.org.    172800 IN      A       199.19.57.1
```

Glue records

How many answers?
How many additional records?

(authoritative for org.)

```
$ dig @199.19.54.1 www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39912
;; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.freebsd.org.               IN      A

;; AUTHORITY SECTION:
freebsd.org.            86400   IN      NS      ns1.isc-sns.net.
freebsd.org.            86400   IN      NS      ns2.isc-sns.com.
freebsd.org.            86400   IN      NS      ns3.isc-sns.info.
```

(authoritative for freebsd.org.)

How many answers?
How many authoritative records?
How many additional records?

```
$ dig @ns1.isc-sns.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17037
;; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.freebsd.org.               IN      A

;; ANSWER SECTION:
www.freebsd.org.        3600    IN      A       69.147.83.33

;; AUTHORITY SECTION:
freebsd.org.            3600    IN      NS      ns2.isc-sns.com.
freebsd.org.            3600    IN      NS      ns1.isc-sns.net.
freebsd.org.            3600    IN      NS      ns3.isc-sns.info.

;; ADDITIONAL SECTION:
ns1.isc-sns.net.        3600    IN      A       72.52.71.1
ns2.isc-sns.com.        3600    IN      A       38.103.2.1
ns3.isc-sns.info.       3600    IN      A       63.243.194.1
```

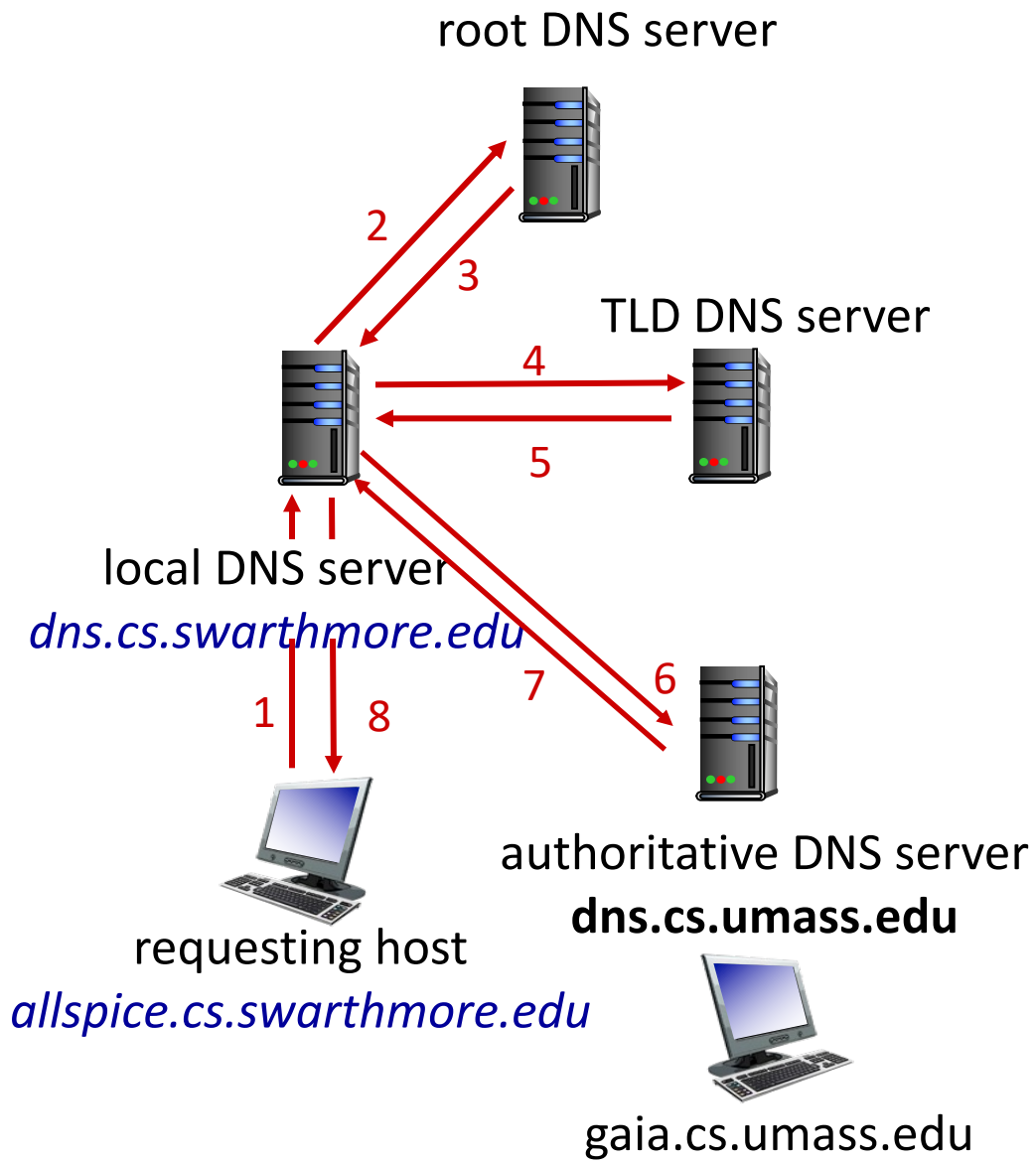
DNS security

DNS Vulnerabilities:

- No authentication
- Connectionless transport layer protocol (UDP)

DNS Attacks:

- Amplification Attack
- Cache Poisoning
- Man-in-the-middle
- DNS Redirection
- DDoS
- DNS Injection



Attacking DNS

DDoS attacks

- Bombard root servers with traffic
  - Not successful to date
  - Traffic Filtering
  - Local DNS servers cache IPs of TLD servers, bypassing root
- Bombard TLD servers
  - Potentially more dangerous

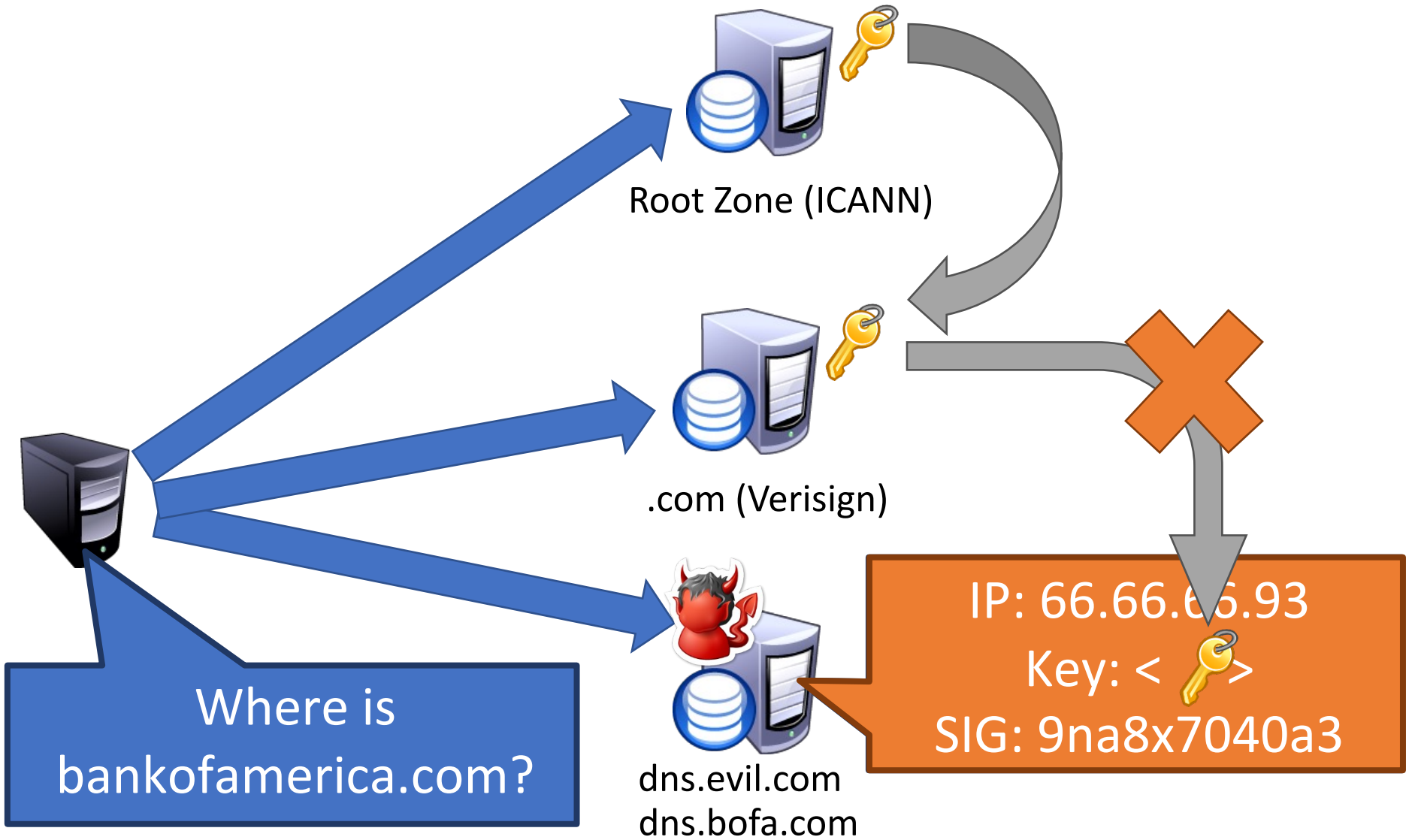
Redirect attacks

- Man-in-middle
  - Intercept queries
- DNS poisoning
  - Send bogus replies to DNS server that caches

Exploit DNS for DDoS

- Send queries with spoofed source address: target IP
- Requires amplification

DNSSEC Hierarchy of Trust



Solution: DNSSEC

- Cryptographically sign critical resource records
  - Resolver can verify the cryptographic signature
- Two new resource types
  - Type = DNSKEY
    - Name = Zone domain name
    - Value = Public key for the zone
  - Type = RRSIG
    - Name = (type, name) tuple, i.e. the query itself
    - Value = Cryptographic signature of the query results

Creates a hierarchy of trust within each zone

Prevents hijacking and spoofing